

# Properties of Conjugate Channels with Applications to Additivity and Multiplicativity

Christopher King

Department of Mathematics, Northeastern University, Boston MA 02115  
king@neu.edu

Keiji Matsumoto

National Institute of Informatics  
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan  
and

ERATO Quantum Computation and Information Project, JST  
Danai Hongo White Bldg, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan  
keiji@nii.ac.jp

Michael Nathanson

Department of Mathematics, Kenyon College, Gambier, OH 43022  
nathansonm@kenyon.edu

Mary Beth Ruskai

Department of Mathematics, Tufts University, Medford, MA 02155  
Marybeth.Ruskai@tufts.edu

February 1, 2008

*Dedicated to the memory of John T. Lewis*

## Abstract

Quantum channels can be described via a unitary coupling of system and environment, followed by a trace over the environment state space. Taking the trace instead over the system state space produces a different mapping which we call the conjugate channel. We explore the properties of conjugate channels and describe several different methods of construction. In general, conjugate channels map  $M_d \mapsto M_{d'}$  with  $d < d'$ , and different constructions may differ by conjugation with a partial isometry. We show that a channel and its conjugate have the same minimal output entropy and maximal output  $p$ -norm. It then follows that the additivity and multiplicativity conjectures for these measures of optimal output purity hold for a product of channels if and only if they also hold for the product of their conjugates. This allows us to reduce these conjectures to the special case of maps taking  $M_d \mapsto M_{d^2}$  with a minimal representation of dimension at most  $d$ .

We find explicit expressions for the conjugates for a number of well-known examples, including entanglement-breaking channels, unital qubit channels, the depolarizing channel, and a subclass of random unitary channels. For the entanglement-breaking channels, channels this yields a new class of channels for which additivity and multiplicativity of optimal output purity can be established. For random unitary channels using the generalized Pauli matrices, we obtain a new formulation of the multiplicativity conjecture. The conjugate of the completely noisy channel plays a special role and suggests a mechanism for using noise to transmit information.

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Basic definitions and results</b>	<b>5</b>
2.1	Construction of conjugate channels . . . . .	5
2.2	Optimal output purity . . . . .	7
<b>3</b>	<b>Conjugates of entanglement breaking maps</b>	<b>10</b>
<b>4</b>	<b>Conjugates of Pauli diagonal channels</b>	<b>13</b>
4.1	Basic set-up . . . . .	13
4.2	Generalized Pauli bases . . . . .	15

4.3	Representations of density matrices . . . . .	17
4.4	Image of the completely noisy conjugate . . . . .	19
4.5	Upper bound on $\nu_p(\Phi)$ . . . . .	22
4.6	Applications to Multiplicativity . . . . .	24
<b>5</b>	<b>Giovannetti-Lloyd linearization operators</b>	<b>26</b>
<b>A</b>	<b>Representations of CPT maps</b>	<b>28</b>
<b>B</b>	<b>Qubit channels</b>	<b>31</b>

# 1 Introduction

The underlying model of noise in a quantum system regards the original system (typically called Alice) as a subsystem of a larger system which includes both the original system and the environment, which we call Bob. We assume that Alice and Bob initially prepare their systems separately after which they evolve in time according to the unitary group of the Hamiltonian of the combined system. Either system can be described at a later time by taking a partial trace over the other. Typically, the unitary interaction entangles the two systems so that each subsystem is in a mixed state. In the most common scenario, Alice can prepare a variety of different states, but Bob always uses the same state  $|\phi\rangle\langle\phi|$ . The map which takes Alice's state  $|\psi\rangle\langle\psi|$  to  $\text{Tr}_B U(t)|\psi \otimes \phi\rangle\langle\psi \otimes \phi|U(t)^\dagger \equiv \Phi(|\psi\rangle\langle\psi|)$  at a fixed time  $t$  is called a channel  $\Phi$ . Taking  $\text{Tr}_A U(t)|\psi \otimes \phi\rangle\langle\psi \otimes \phi|U(t)^\dagger$  defines a map  $\Phi^C$  whose output is a state  $\Phi^C(|\psi\rangle\langle\psi|)$  which describes the information available to Bob at the same fixed time  $t$ . We call this map the *conjugate channel*.

Mathematically, both  $\Phi$  and  $\Phi^C$  are completely positive trace-preserving (CPT) maps. The former takes  $\mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_A)$  and the latter  $\mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_B)$  where  $\mathcal{H}_A$  and  $\mathcal{H}_B$  denote the Hilbert spaces of Alice and Bob respectively. In this paper we develop the properties of conjugate channels for CPT maps when both Hilbert spaces are finite dimensional. We study the conjugates of several classes of channels, including entanglement-breaking (EBT) maps and a higher-dimensional analog of the qubit unital channels, which we call Pauli-diagonal. Conjugate channels have been studied before in other settings including Appendix B of [4] and [37]. After completion of this work, we learned that much of our analysis of conjugate maps was done independently by Holevo [14] for maps which are completely positive, but

not necessarily trace-preserving. Holevo obtains most of the results in Sections 2 and 3, with the exception of our Theorem 6. He also obtains a result similar to Corollary 11.

Although the channels  $\Phi$  and  $\Phi^C$  are quite different in general, for any pure input state  $|\psi\rangle$  the two output states  $\Phi(|\psi\rangle\langle\psi|)$  and  $\Phi^C(|\psi\rangle\langle\psi|)$  must have the same nonzero spectrum. This means that the channels  $\Phi$  and  $\Phi^C$  have the same maximal output  $p$ -norms  $\nu_p(\Phi) = \sup_\rho \|\Phi(\rho)\|_p = \nu_p(\Phi^C)$ , and also the same minimal output entropy. We show that for any pair of channels, the additivity and multiplicativity conjectures for these measure of optimal output purity hold if and only if the same conjecture holds for their conjugate channels. For example

$$\nu_p(\Phi_1 \otimes \Phi_2) = \nu_p(\Phi_1)\nu_p(\Phi_2) \iff \nu_p(\Phi_1^C \otimes \Phi_2^C) = \nu_p(\Phi_1^C)\nu_p(\Phi_2^C). \quad (1)$$

This equivalence allows to obtain some new results about these conjectures. One of these is the realization that it would suffice to prove them for the special class of maps taking  $M_d \mapsto M_{d^2}$  with a minimal representation of dimension at most  $d$ .

This work was motivated by the observation of a similarity between King's proofs of multiplicativity [20] for EBT maps and for Hadamard diagonal channels [21] which seemed to suggest a kind of duality. The concept of conjugate channels allows us to make this duality explicit when the EBT map belongs to a subclass we call extreme CQ and the Hadamard diagonal channel is also trace-preserving.

A large part of the paper considers channels which are convex combinations of unitary conjugations of the generalized Pauli matrices; we will call these channels Pauli diagonal. We show that the image of the conjugate of the completely noisy channel is essentially equivalent to the original state, i.e., when the noise completely destroys Alice's state, Bob can recover it. We also show that the conjugate of a Pauli diagonal channel can be written as the composition of a simple Hadamard channel (using only one diagonal Kraus operator) with the conjugate of the completely noisy map. This allows a simple and appealing reformulation of the multiplicativity conjecture for these channels. Although it has not yet led to a proof, this approach provides some new insights.

The paper is organized as follows. In Section 2 we define the conjugate of a channel, show how to use its Kraus representation to construct its conjugate and show that it is well-defined up to a partial isometry. We also prove the equivalence of the multiplicativity problem for a product of channels and their conjugates, and a reduction theorem. In Section 3 we study the conjugates of EBT channels, and extend King's results [21] about Hadamard diagonal channels to a larger class, which we call simply Hadamard channels. In Section 4 we study the Pauli diagonal channels and several related classes of random unitary channels. In Section 5

we derive a relation between the conjugate channels and the Giovannetti-Lloyd linearization operators which arose in the study of multiplicativity for integer values of  $p$  [9]. Appendix A summarizes some basic results about representations of channels and extends them to the less familiar situations of maps between spaces of different dimension and equivalence via partial isometries. Appendix B gives a detailed analysis of the issues which arise for the Pauli diagonal channels in the case of unital qubit maps.

## 2 Basic definitions and results

### 2.1 Construction of conjugate channels

We begin with two well-known representations of a CPT map  $\Phi : M_d \mapsto M_{d'}$ . The Lindblad-Stinespring (LS) ancilla representation [35, 26] can be written as

$$\Phi(\rho) = \text{Tr}_C U (\rho \otimes |\phi\rangle\langle\phi|) U^\dagger \quad (2)$$

where  $|\phi\rangle$  is a pure state on an auxiliary space  $\mathcal{H}_C$ , and  $U : \mathbb{C}^d \otimes \mathcal{H}_C \mapsto \mathbb{C}^{d'} \otimes \mathcal{H}_C$  is a partial isometry. We denote the minimal dimension for the auxiliary space  $\mathcal{H}_C$  as  $\kappa$  and note that  $\kappa \leq dd'$ . There is no loss of generality in assuming that the rank of  $U$  is  $d_\kappa$ , and we will always assume that  $d_C = \dim \mathcal{H}_C < \infty$ . However, we will not restrict ourselves to minimal representations.

The standard operator-sum or Kraus-Choi representation of  $\Phi$  is [23]

$$\Phi(\rho) = \sum_{k=1}^{d_C} F_k \rho F_k^\dagger \quad (3)$$

where the operators satisfy the trace-preserving condition  $\sum F_k^\dagger F_k = I$ . As discussed in Appendix A, these two representations can be connected by the relation  $F_k = \text{Tr}_C [U(I \otimes |\phi\rangle\langle e_k|)]$ . Moreover, different Kraus representations can be related a by partial isometry  $W$  of rank  $\kappa$  as explained after (92).

Using the representation (2), we construct the *conjugate channel*  $\Phi^C : M_d \mapsto M_{d_C}$  as

$$\Phi^C(\rho) = \text{Tr}_B U (\rho \otimes |\phi\rangle\langle\phi|) U^\dagger \quad (4)$$

where we identify  $\mathcal{H}_B = \mathbb{C}^{d'}$ . To see how (4) arises from the Kraus representation (3), define

$$\mathbf{F}(\rho) = \sum_{jk} |e_j\rangle\langle e_k| \otimes F_j \rho F_k^\dagger \in M_{d_C} \otimes M_{d'} \quad (5)$$

Then  $\Phi(\rho) = \text{Tr}_C \mathbf{F}(\rho)$ , and the conjugate channel can be written as

$$\Phi^C(\rho) = \text{Tr}_B \mathbf{F}(\rho) = \sum_{jk} \text{Tr} \left( F_j \rho F_k^\dagger \right) |e_j\rangle\langle e_k|. \quad (6)$$

The channel (6) can itself be written in a Kraus representation

$$\Phi^C(\rho) = \sum_{\mu=1}^{d'} R_\mu \rho R_\mu^\dagger \quad (7)$$

where the Kraus operators satisfy

$$(R_\mu)_{jk} = (F_j)_{\mu k} \quad (8)$$

Two sets of Kraus operators related as in (8) will also be called *conjugate*.

For a given channel  $\Phi$ , there are many choices possible for  $\mathcal{H}_C$ ,  $|\phi\rangle$  and  $U$  in (2). We denote by  $\mathcal{C}(\Phi)$  the collection of all conjugate channels defined as in (4) using all representations of the same channel  $\Phi$ . The following Lemma shows that these different representations are related by conjugation with a partial isometry.

**Lemma 1** *For any pair of elements  $\Phi^{C_1}, \Phi^{C_2} \in \mathcal{C}(\Phi)$  one can find a partial isometry  $W$  of rank  $\kappa$  such that*

$$\Phi^{C_1} = \Gamma_W \circ \Phi^{C_2} \quad \text{and} \quad \Phi^{C_2} = \Gamma_{W^\dagger} \circ \Phi^{C_1} \quad (9)$$

where  $\Gamma_W(\rho) = W\rho W^\dagger$ .

**Proof:** Let  $\{F_k\}$  and  $\{G_m\}$  be Kraus representations for  $\Phi$  so that

$$\Phi(\rho) = \sum_k F_k \rho F_k^\dagger = \sum_m G_m \rho G_m^\dagger \quad (10)$$

and the corresponding conjugate representations can be written as

$$\Phi^{C_1}(\rho) = \sum_{\mu}^{d'} R_\mu \rho R_\mu^\dagger, \quad \Phi^{C_2}(\rho) = \sum_{\mu}^{d'} S_\mu \rho S_\mu^\dagger. \quad (11)$$

with  $R_\mu, S_\mu$  given by (8). As explained after (92), there is a partial isometry  $W$  of rank  $\kappa$  such that  $F_k = \sum_m w_{km} G_m$ . Then (8) implies that  $R_\mu = W S_\mu$  so that

$$\Phi^{C_1}(\rho) = \sum_{\mu} R_\mu \rho R_\mu^\dagger = W \left( \sum_{\mu} S_\mu \rho S_\mu^\dagger \right) W^\dagger = W \Phi^{C_2}(\rho) W^\dagger \quad (12)$$

If, in addition,  $\{G_m\}$  is minimal, then  $W^\dagger W = I_\kappa$ , and it follows immediately that  $\Phi^{C_2}(\rho) = W^\dagger \Phi^{C_1}(\rho) W$ . If neither representation is minimal, we can use the fact proved after (92) that  $G_m = \sum_j \bar{w}_{jm} F_j$  which implies  $S_\mu = W^\dagger R_\mu$  **QED**

In most of our applications and results, the particular choice of element in  $\mathcal{C}(\Phi)$  will be irrelevant, and we will generally speak of “the” conjugate channel  $\Phi^C$  with the understanding that it is unique up to the partial isometry described above. With this understanding we note that the conjugate of the conjugate is the original channel, that is  $(\Phi^C)^C = \Phi$ , or  $\Phi \in \mathcal{C}(\Phi^C)$ .

Another method of representing a channel is via its Choi-Jamiołkowski (CJ) matrix (88) which gives a one-to-one correspondence between CP maps  $\Phi : M_d \mapsto M_{d'}$  and positive semi-definite matrices on  $M_d \otimes M_{d'}$ . The subset which satisfies  $\text{Tr}_B \Gamma_{AB} = \frac{1}{d} I_d$  gives the CPT maps. The next result gives a relation between the CJ matrix of a channel and its conjugate.

**Proposition 2** *Let  $\Phi$  be a CPT map with CJ matrix  $\Gamma_{AB} = (I \otimes \Phi)(|\phi\rangle\langle\phi|)$  as in (88) and let  $\Gamma_{ABC}$  be a purification of  $\Gamma_{AB}$ . Then  $\Gamma_{AC} = \text{Tr}_B \Gamma_{ABC}$  is the CJ matrix of the conjugate channel  $\Phi^C$ .*

The proof, which is given in Appendix A, is a consequence of the fact that the eigenvectors of the CJ matrix generate a minimal set of Kraus operators. Although this approach may seem less constructive, in some contexts (see work of Horodecki), channels are naturally defined in terms of their CJ matrix or “state representation”. Moreover, this approach has less ambiguity. If the standard basis for  $\mathcal{H}_C$  is used and  $\Gamma_{AB}$  has non-degenerate eigenvalues, it is unique up to a permutation. More generally, if one labels the eigenvalues of  $\Gamma_{AB}$  in increasing (or decreasing) order and labels the basis for  $\mathcal{H}_C$  accordingly, then  $\Gamma_{AC}$  is unique up to conjugation with a unitary matrix of the form  $I_A \otimes U_C$  where  $U_C$  is a unitary matrix which is block diagonal corresponding to the degeneracies of  $\Gamma_{AB}$ .

## 2.2 Optimal output purity

Our first result, although straightforward, is a key ingredient, so we state and prove it explicitly here.

**Theorem 3** *The output  $\Phi(|\psi\rangle\langle\psi|)$  of a channel acting on a pure state has the same non-zero spectrum as the output  $\Phi^C(|\psi\rangle\langle\psi|)$  of its conjugate acting on the same pure state.*

**Proof:** Let  $\gamma_{AB} = U(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|)U^\dagger = |\Psi_{AB}\rangle\langle\Psi_{AB}|$  with  $U, |\phi\rangle$  as in (2) and  $|\Psi_{AB}\rangle = U(|\psi\rangle \otimes |\phi\rangle)$ . Then  $\gamma_{AB}$  is a pure state,  $\Phi(|\psi\rangle\langle\psi|) = \gamma_A = \text{Tr}_B \gamma_{AB}$  and  $\Phi^C(|\psi\rangle\langle\psi|) = \gamma_B = \text{Tr}_A \gamma_{AB}$ . The result then follows from the well-known fact that the reduced density matrices of a pure state have the same non-zero spectrum. **QED**

As an immediate corollary, it follows that a channel  $\Phi$  and its conjugate  $\Phi^C$  always have the same maximal output purity and minimal output entropy. Recall that the maximal output purity is defined for  $p \geq 1$  by

$$\nu_p(\Phi) \equiv \sup_{\rho} \|\Phi(\rho)\|_p = \sup_{|\psi\rangle} \|\Phi(|\psi\rangle\langle\psi|)\|_p \quad (13)$$

and the minimal output entropy is

$$S_{\min}(\Phi) \equiv \inf_{\rho} S(\Phi(\rho)) = \inf_{|\psi\rangle} S(\Phi(|\psi\rangle\langle\psi|)), \quad (14)$$

where the sup and inf are taken over normalized states  $\rho$  and  $|\psi\rangle$ .

**Corollary 4** *For any CPT map  $\Phi$ ,  $\nu_p(\Phi) = \nu_p(\Phi^C)$  and  $S_{\min}(\Phi) = S_{\min}(\Phi^C)$ .*

For any pair of conjugate channels  $\Phi_1^C$  and  $\Phi_2^C$ , the product  $\Phi_1^C \otimes \Phi_2^C$  is again a channel, and from the definition (4) it follows that  $\Phi_1^C \otimes \Phi_2^C \in \mathcal{C}(\Phi_1 \otimes \Phi_2)$ . Therefore given any representative  $[\Phi_1 \otimes \Phi_2]^C$  there is a partial isometry  $W$  such that

$$[\Phi_1 \otimes \Phi_2]^C = \Gamma_W \circ [\Phi_1^C \otimes \Phi_2^C] \quad (15)$$

Combining Corollary 4 and (15) implies the equivalence of the additivity and multiplicativity problems for channels and their conjugates. For convenience we restate the result below in Theorem 5.

$$\nu_p(\Phi_1 \otimes \Phi_2) = \nu_p(\Phi_1) \nu_p(\Phi_2) \quad (16)$$

$$S_{\min}(\Phi_1 \otimes \Phi_2) = S_{\min}(\Phi_1) + S_{\min}(\Phi_2) \quad (17)$$

**Theorem 5** *For any pair of channels  $\Phi_1, \Phi_2$ , and any  $p \geq 1$ , (16) holds if and only if*

$$\nu_p(\Phi_1^C \otimes \Phi_2^C) = \nu_p(\Phi_1^C) \nu_p(\Phi_2^C),$$

*and (17) holds if and only if*

$$S_{\min}(\Phi_1^C \otimes \Phi_2^C) = S_{\min}(\Phi_1^C) + S_{\min}(\Phi_2^C)$$



There are also additivity conjectures for the entanglement of formation (EoF) and Holevo capacity  $C_{\text{Holv}}(\Phi)$ . For a bipartite state  $\gamma_{AC}$ , define

$$\text{EoF}(\gamma_{AC}) = \inf \left\{ \sum_j \pi_j S[\text{Tr}_C |\psi_j\rangle\langle\psi_j|] : \sum_j \pi_j |\psi_j\rangle\langle\psi_j| = \gamma_{AC} \right\}. \quad (18)$$

Following [28] and [34], we use (2) to associate  $\gamma_{AC}$  with  $\Phi$  and a state  $\rho$  (as in the proof of Theorem 3) so that  $\Phi(\rho) = \text{Tr}_C \gamma_{AC}$ . Then we define  $\chi[\Phi(\rho)] = S[\Phi(\rho)] - \text{EoF}(\gamma_{AC})$  and  $C_{\text{Holv}}(\Phi) = \sup_{\rho} \chi[\Phi(\rho)]$ . The additivity conjecture for Holevo capacity is

$$C_{\text{Holv}}(\Phi_1 \otimes \Phi_2) = C_{\text{Holv}}(\Phi_1) + C_{\text{Holv}}(\Phi_2) \quad (19)$$

and the superadditivity conjecture for EoF is

$$\text{EoF}(\gamma_{A_1 C_1 A_2 C_2}) \geq \text{EoF}(\gamma_{A_1 C_1}) + \text{EoF}(\gamma_{A_2 C_2}). \quad (20)$$

Shor [34] has shown that these conjectures are globally equivalent to (17). However, the validity of (17) for some pair of channels need not imply (19) for the same pair, or vice versa. In Theorem 7, we use special features of the channel to prove both separately. Holevo [14] proved the more general result that if (20) holds for a state associated with a pair of channels, then it also holds for their conjugates.

Theorem 5 allows one to extend known results on additivity and multiplicativity to their conjugates. Conversely, if one can prove these conjectures for some class of conjugate channels, then one can obtain new results about the original class. The new results obtained thus far are quite modest. This may be partly because the conjugate channels typically take  $M_d \mapsto M_{d'}$  with  $d' > d$ , and channels of this type have not been studied as extensively. The next result shows that it would suffice to prove multiplicativity for a very small and special subset of these maps.

**Theorem 6** *Suppose that (16) holds for all tensor products  $\Psi_1 \otimes \Psi_2$  of CPT maps with  $\Psi_i : M_{d_i} \mapsto M_{d_i d'_i}$  whose minimal representation has dimension  $\kappa_i \leq d'_i$ . Then the multiplicativity conjecture (16) holds for all tensor products of CPT maps  $\Phi_1 \otimes \Phi_2$  with  $\Phi_i : M_{d_i} \mapsto M_{d'_i}$ .*

**Proof:** First, let  $\kappa_i$  be the minimum number of Kraus operators needed to represent  $\Phi_i$  and consider the typical case  $\kappa_i = d_i d'_i$ . Then  $\Phi_i^C : M_{d_i} \rightarrow M_{d_i d'_i}$ , but by (8) requires only  $d'_i$  Kraus operators. Thus, under the hypothesis of the theorem, (16) holds for  $\Phi_1^C \otimes \Phi_2^C$ . But then by Theorem 5, (16) also holds for  $\Phi_1 \otimes \Phi_2$ . When the number of Kraus operators is less than  $d_i d'_i$ , one can simply use a redundant

representation with  $d_i d'_i$  operators. Alternatively, one could perturb the channel to  $(1 - \epsilon)\Phi_i + \epsilon N$ , with  $N$  the completely noisy map, and then let  $\epsilon \rightarrow 0$ . **QED**

Choi showed that a CPT map whose Kraus operators  $F_j$  generate a linearly independent set  $F_j^\dagger F_k$  in  $M_{d'}$  is an extreme point in the set of all CPT maps. Since,  $M_{d'}$  is a vector space of dimension  $(d')^2$ , this implies that any extreme point can be represented using at most  $d'$  Kraus operators. In [31] maps which require at most  $d'$  Kraus operators, but are not true extreme points, are called *quasi-extreme* and all those whose minimal representation has rank  $\kappa \leq d'$  generalized extreme points. From a geometric point of view, this extends the extreme points to include some hyperplanes in regions where the boundary of the convex set of CPT maps is flat. For qubit maps, the quasi-extreme points are convex combinations of conjugations with two Pauli matrices; these maps correspond to edges of the tetrahedron of unital qubit maps.

It was shown in [31] that any qubit map which is a generalized extreme point has at least two pure output states. For such maps, (16) is trivial. However, using Theorem 6 to prove multiplicativity for all qubit maps, requires proving (16) for all maps  $\Phi : M_2 \mapsto M_4$  which can be written using two Kraus operators.

For  $d > 2$ , there are extreme points which do not have pure outputs. In particular, when  $d = 3$ , the Werner-Holevo (WH) counter-example map [36] is an extreme CPT map, but all pure states are mapped into projections of rank 2. (Note that the WH map is not even quasi-extreme when  $d \geq 4$ .) Finding all generalized extreme points of CPT maps is a difficult problem which has not yet been solved, even for maps taking  $M_3 \mapsto M_3$ . Using (8) it would suffice to find all maps taking  $M_3 \mapsto M_d$  for  $d \leq 9$  whose CJ matrix has rank  $\leq 3$ .

A non-extreme map  $\Phi : M_d \mapsto M_d$  can have minimal dimension  $d^2$ ; its conjugate  $\Phi^C : M_d \mapsto M_{d^2}$  has a CJ matrix which is  $d^3 \times d^3$ . For general maps  $\Psi : M_d \mapsto M_{d^2}$  there are extreme points with minimal dimension  $d^2$ , but only those with minimal dimensions  $d$  arise from conjugates in this way. The reduction in Theorem 6 to generalized extreme points with CJ matrix of rank at most  $d$  rather than  $d^2$  is quite remarkable.

### 3 Conjugates of entanglement breaking maps

In this section we review the class of entanglement-breaking maps. An entanglement-breaking trace-preserving (EBT) map [33] is a CPT map  $\Phi$  for which  $(I \otimes \Phi)(\rho)$  is

separable for all  $\rho$ . A number of equivalent criteria are known [16], e.g.,

$$\Phi(\rho) = \sum_m R_m \text{Tr } E_b \rho \quad (21)$$

where  $\{E_b\}$  is a POVM and each  $R_m$  is a density matrix. This is the form introduced by Holevo [12]. Here, we use the fact that any EBT map can be written using Kraus operators  $F_k = |x_k\rangle\langle w_k|$  with rank one. Then

$$\Phi(\rho) = \sum_k |x_k\rangle\langle x_k| \langle w_k| \rho |w_k\rangle, \quad (22)$$

and  $\sum_k \langle x_k|x_k\rangle |w_k\rangle\langle w_k| = I$ . Using the notation of (5),

$$\mathbf{F}(\rho) = \sum_{jk} |e_j\rangle\langle e_k| \otimes |x_j\rangle\langle x_k| \langle w_j| \rho |w_k\rangle \quad (23)$$

and it follows that

$$\Phi^C(\rho) = \sum_{jk} |e_j\rangle\langle e_k| \langle x_j|x_k\rangle \langle w_j| \rho |w_k\rangle = X * W_\rho \quad (24)$$

where  $*$  denotes the Hadamard product,  $X$  is the matrix with elements  $\langle x_j|x_k\rangle$  and  $W_\rho$  is the matrix with elements  $\langle w_j|\rho|w_k\rangle$ , which can be viewed as a non-standard “representative” of  $\rho$ . Thus in general the conjugate of an EBT map need not itself be an EBT map. If we choose  $c_{jm}$  such that  $CC^\dagger = X$  then the Kraus operators for (24) can be written in the form

$$R_m = \sum_j c_{jm} |e_j\rangle\langle w_j| \quad (25)$$

where  $\{|e_j\rangle\}$  are orthonormal, but  $\{|w_j\rangle\}$  need not be. Conversely, suppose that the Kraus operators of a map  $\Phi$  have the form (25) with  $\{e_j\}$  orthonormal. Then a straightforward calculation shows that  $\Phi^C$  is an EBT map.

A special case of (22) arises when the  $w_k$  form an orthonormal basis. In this case  $\Phi$  is called a classical-quantum or CQ channel. Moreover, the fact that  $|x_k\rangle\langle x_k|$  are rank one implies that  $\Phi$  is an extreme point of the set of CPT maps and hence an extreme point of the set of EBT maps [16]. From (24) it follows that  $W_\rho$  is the usual matrix representative of  $\rho$  in the O.N. basis  $w_k$  so that  $\Phi^C(\rho) = X * \rho$ . Since  $X$  is positive semidefinite this implies that  $\Phi^C$  has simultaneously diagonal Kraus operators, and one can easily see from (25) that this is the case when the  $w_k$  are orthonormal. This class of channels was introduced in [25] where it was

called “diagonal”. We prefer to call them “Hadamard channels” or “Hadamard diagonal” maps.<sup>1</sup> Thus, the conjugate of an extreme CQ channel is a Hadamard diagonal channel. King [17, 21] has shown that both CQ channels and arbitrary (not necessarily trace-preserving) Hadamard diagonal CP maps satisfy the multiplicativity (16) for all  $p$ . Since this holds trivially for both extreme CQ channels and Hadamard diagonal CPT maps, we do not obtain a new result.

To get a better understanding of the general case, note that an arbitrary  $d' \times d$  matrix, or operator  $Q : \mathbf{C}^d \mapsto \mathbf{C}^{\kappa}$ , can be written as

$$Q = \sum_{jk} a_{jk} |e_j\rangle \langle e'_k| = \sum_j |e_j\rangle \langle w_j|$$

with  $|w_j\rangle = \sum_k a_{jk} |e'_k\rangle$ . Thus, the restriction in (25) which distinguishes  $\Phi^C$  from an arbitrary channel is that the vectors  $w_k$  are the same for all Kraus operators. The POVM requirement that  $\sum_{k=1}^{\kappa} |w_k\rangle \langle w_k| = I_d$  in (22) implies that  $\{|w_k\rangle\}$  are orthonormal when  $\kappa = d$ ; this is precisely the CQ case discussed above. In the general case, we can use Theorem 5 to obtain the following result, which extends King’s results in [19] to CPT maps with  $\kappa > d$ .

**Theorem 7** *Let  $\Phi_1 : M_d \mapsto M_{\kappa}$  be a CPT map with the Hadamard form (24) or, equivalently, a Kraus representation of the form (25). Then for any CPT map  $\Phi_2$ , the multiplicativity (16) holds for all  $p \geq 1$ , the additivity of minimal output entropy (17) holds, and additivity of Holevo capacity (19) holds.*

**Proof:** The first part of the theorem follows immediately from Theorem 5, the fact that any channel satisfying the hypothesis can be written as the conjugate of an EBT map, and the fact that EBT maps satisfy (17) [33] and (16) [19]. To prove (19), use (2) to define  $\gamma_{AC}$  as before (18). Since each  $|\psi_j\rangle \langle \psi_j|$  in (18) is a pure state,  $S[\text{Tr}_C |\psi_j\rangle \langle \psi_j|] = S[\text{Tr}_A |\psi_j\rangle \langle \psi_j|]$  and it follows immediately that

$$\text{EoF}(\gamma_{AC}) = S[\Phi(\rho)] - \chi[\Phi(\rho)] = S[\Phi^C(\rho)] - \chi[\Phi^C(\rho)] \quad (26)$$

If  $\gamma_{A_1 C_1 A_2 C_2}$  is associated with a state  $\rho_{12}$  using the product representation (2) for a pair of channels and any one of  $\Phi_1, \Phi_2, \Phi_1^C, \Phi_2^C$  is EBT, then (20) holds. (This result follows immediately from eqn. (25) in [33], as noted in [5]; the same result appears in Lemma 3 of [18]). Now let  $\rho_{12}$  achieve the supremum in

$$C_{\text{Holv}}(\Phi_1 \otimes \Phi_2) = \sup_{\rho_{12}} \chi[(\Phi_1 \otimes \Phi_2)(\rho_{12})] \quad (27)$$

---

<sup>1</sup>The term “diagonal channel” seems to be a natural choice for a different class of channels, namely those whose matrix representative in a particular basis is diagonal. In Section 4 we consider a class which seems natural to call Pauli diagonal channels.

Then, as shown in [28], it follows from (20) and the subadditivity of entropy that

$$C_{\text{Holv}}(\Phi_1 \otimes \Phi_2) \leq C_{\text{Holv}}(\Phi_1) + C_{\text{Holv}}(\Phi_2)$$

Since the reverse inequality is trivial, (19) holds. **QED**

## 4 Conjugates of Pauli diagonal channels

### 4.1 Basic set-up

In this section we consider a subclass of convex combinations of unitary conjugations that can be regarded as the generalization to  $d$ -dimensions of the unital qubit channels.

In the case of a unital qubit channel we can assume, without loss of generality, that  $\Phi(\rho) = \sum_{k=0}^3 a_k \sigma_k \rho \sigma_k$  where  $a_k \geq 0$ ,  $\sum_k a_k = 1$  and  $\sigma_k$  are the usual Pauli matrices, with the convention that  $\sigma_0 = I$ . One can write a qubit density matrix as

$$\rho = \frac{1}{2}[w_0 I + \mathbf{w} \cdot \boldsymbol{\sigma}] = \frac{1}{2} \sum_{k=0}^3 w_k \sigma_k. \quad (28)$$

where  $w_0 = 1 \geq |\mathbf{w}|^2 = \sum_{k=1}^3 w_k^2$ . Then one can choose  $F_k = \sqrt{a_k} \sigma_k$  and

$$\Phi^C(\rho) = \sqrt{A} \begin{pmatrix} w_0 & w_1 & w_2 & w_3 \\ w_1 & w_0 & -iw_3 & iw_2 \\ w_2 & iw_3 & w_0 & -iw_1 \\ w_3 & -iw_2 & iw_1 & w_0 \end{pmatrix} \sqrt{A} = 4\sqrt{A} N^C(\rho) \sqrt{A} \quad (29)$$

where  $A$  is the diagonal matrix with elements  $a_j \delta_{jk}$  and  $N^C$  is the conjugate of the completely noisy map for which all  $a_k = \frac{1}{4}$ .

To generalize this to dimension  $d > 2$ , we first observe that any orthonormal basis for  $M_d$  yields a set of Kraus operators for the completely noisy channel. (To see this note that  $E_{jk} = |j\rangle\langle k|$  is a set of Kraus operators satisfying  $\text{Tr } E_{ik}^\dagger E_{j\ell} = \delta_{ij} \delta_{k\ell}$ , and that any orthonormal basis is unitarily equivalent to  $\{E_{jk}\}$ .) Let  $\mathcal{T}$  denote such a basis with the additional requirement that every element is unitary and the first is the identity, i.e.,

$$\mathcal{T} = \{T_m : T_0 = I, \text{Tr } T_m^\dagger T_n = d\delta_{mn}, T_m^\dagger T_m = I, m = 0, 1 \dots d^2 - 1\} \quad (30)$$

Then these operators generate the completely noisy channel via

$$\frac{1}{d^2} \sum_{m=0}^{d^2-1} T_m \rho T_m^\dagger = (\text{Tr } \rho) \frac{1}{d} I \equiv N(\rho). \quad (31)$$

Now consider channels

$$\Phi(\rho) = \sum_{m=0}^{d^2-1} a_m T_m \rho T_m^\dagger \quad (32)$$

with  $a_m \geq 0$ ,  $\sum_m a_m = 1$ . The Kraus operators for this channel are  $F_m = \sqrt{a_m} T_m$ . One then finds

$$\begin{aligned} \Phi^{C,T}(\rho) &= \sum_{mn} |e_m\rangle \langle e_n| \sqrt{a_m a_n} \text{Tr } T_m \rho T_n^\dagger \\ &= d^2 \sqrt{A} N^{C,T}(\rho) \sqrt{A} = d^2 |\alpha\rangle \langle \alpha| * N^{C,T}(\rho) \end{aligned} \quad (33)$$

where  $A$  is the diagonal matrix with elements  $a_m \delta_{mn}$ ,  $|\alpha\rangle$  is the vector with elements  $\sqrt{a_m}$ , and we use the superscript  $\mathcal{T}$  to emphasize that  $N^{C,T}$ , the conjugate of the completely noisy channel, is constructed using a specific choice for the set of Kraus operators. Thus, the conjugate of a channel of the form (32) can be written as the composition  $\Phi^{C,T} = \Psi \circ N^{C,T}$  with  $\Psi$  a Hadamard diagonal channel with a single Kraus operator,  $\sqrt{A}$ .

Now define  $\mathcal{N}^T = \{N^{C,T}(\rho) : \rho = |\psi\rangle \langle \psi|\}$  to be the image of the conjugate of the completely noisy channel acting on pure states. Then Corollary 4 allows us to rewrite the maximal  $p$ -norm as a variation over elements of  $\mathcal{N}^T$ .

**Theorem 8** *Let  $\Phi$  be a channel of the form (32) in the basis  $\mathcal{T}$ . Then*

$$\nu_p(\Phi) = d^2 \sup_{\gamma \in \mathcal{N}^T} \|\sqrt{A} \gamma \sqrt{A}\|_p = d^3 \sup_{\gamma \in \mathcal{N}^T} \|\gamma A \gamma\|_p \quad (34)$$

where  $A$  is the diagonal matrix with elements  $a_m \delta_{mn}$ .

**Proof:** For all  $\gamma \in \mathcal{N}^T$ , it follows from Theorem 3 that the non-zero eigenvalues of  $\gamma$  are  $\frac{1}{d}$  which implies that  $d\gamma$  is a rank  $d$  projection. Therefore,

$$\|\sqrt{A} \gamma \sqrt{A}\|_p = \|\sqrt{\gamma} A \sqrt{\gamma}\|_p = d \|\gamma A \gamma\|_p$$

Then (34) follows from Corollary 4. **QED**

Despite the apparent simplicity of (34) and the expressions for  $\Phi^{C,T}$  above, it is not easy to exploit Theorem 8. In order to do so, we need to choose a specific basis and obtain more information about the set  $\mathcal{N}^T$ .

## 4.2 Generalized Pauli bases

We will be particularly interested in bases  $\mathcal{T}$  which satisfy (30) and have the additional property that

$$T_m^\dagger T_n = e^{i\phi_{kmn}} T_k \quad (35)$$

where  $k$  depends on  $m, n$ . In this case,  $\text{Tr } T_m \rho T_n^\dagger = e^{-i\phi_{kmn}} \text{Tr } T_k \rho$  so that each row of  $N^{C,T}(\rho)$  is determined by permuting the elements of the first row after multiplication by suitable phase factors. When  $\mathcal{T}$  has the property that  $T_m \in \mathcal{T} \Rightarrow T_m^\dagger = T_{m'} \in \mathcal{T}$  then one can interpret (35) as defining a group operation on  $\mathcal{T}$ .

One particular realization of  $T_m$  satisfying (35) is given by the generalized Pauli matrices  $X^j Z^k$ ,  $j, k = 0 \dots d-1$  with  $T_0 = I$ , and, e.g.,  $T_m = X^j Z^k$  for  $m = (d-1)j + k$ . Given a fixed orthonormal basis  $\{|e_i\rangle\}$  for  $\mathbf{C}^d$ , the matrices  $X$  and  $Z$  can be defined by

$$X|e_k\rangle = |e_{k+1}\rangle \quad \text{and} \quad Z|e_k\rangle = e^{2\pi i(k/d)} |e_k\rangle \quad (36)$$

with addition mod  $d$  in the subscript. It will then be convenient to identify  $w_{jk} = v_m$  for  $m = (d-1)j + k$ .

When  $d = d_1 d_2$ , we will also want to consider  $T_m$  which are tensor products of the generalized Pauli matrices, particularly when studying additivity and multiplicativity. Ritter [30] has considered  $T_m$  given by the so-called Gell-mann matrices which arise in the representation theory of  $SU(n)$ .

The generalized Pauli matrices satisfy the commutation relation

$$ZX = e^{i2\pi/d} XZ. \quad (37)$$

It then follows that the matrix representing a channel  $\Phi$  of the form (32) in this basis, is diagonal. In fact

$$\text{Tr} (X^i Z^k)^\dagger \Phi(X^j Z^\ell) = \delta_{ij} \delta_{k\ell} \lambda_{jk} \quad (38)$$

with

$$\lambda_{jk} = e^{jk \frac{2\pi i}{d}} \sum_{mn} e^{(mk-jn) \frac{i2\pi}{d}} a_{mn} = \bar{\lambda}_{d-j, d-k}. \quad (39)$$

Moreover,

$$\Phi : \frac{1}{d} [I + \sum_{jk} w_{jk} X^j Z^k] \mapsto \frac{1}{d} [I + \sum_{jk} \lambda_{jk} w_{jk} X^j Z^k]. \quad (40)$$

We will call channels of the form (32) in the generalized Pauli basis *Pauli diagonal* channels. They are a natural generalization of the unital qubit channels. Pauli diagonal channels are Weyl covariant which implies [3, 13]

$$C_{\text{Holv}}(\Phi) = \log d - S_{\min}(\Phi). \quad (41)$$

Any channel  $\Psi$  can be represented in a basis  $\mathcal{T}$  by the matrix  $X$  with elements  $x_{mn} = \text{Tr } T_m^\dagger \Psi(T_n)$ . When  $\Psi$  is trace-preserving,  $x_{0n} = \delta_{0n}$  and if  $\Psi$  is unital  $x_{m0} = \delta_{m0}$ . In the case of qubits, any unital channel can be diagonalized in the usual Pauli basis by using the singular value decomposition and the correspondence between rotations in  $\mathbf{R}^3$  and unitaries in  $M_2$ . (See [22] for details.) One could, in principle, use the singular value decomposition to diagonalize  $X$ . However, the corresponding change of bases will not normally preserve the properties (30) and (35). Thus, even a convex combination of conjugation with arbitrary unitary conjugations can not necessarily be written in diagonal form using the generalized Pauli basis. In fact, when  $d = d_1 d_2$ , a channel which is diagonal in a tensor product of Pauli bases need not be diagonal in the generalized Pauli basis for  $d$ , and vice versa. (This is easy to check for  $d = 4$ ,  $d_1 = d_2 = 2$ .)

In at least one non-trivial case it is possible to explicitly compute the maximal  $p$ -norm of this class of channels, that is when  $p = 2$  and  $d = 3$ .

**Proposition 9** *The maximal 2-norm of a Pauli diagonal channel satisfies the bound*

$$\nu_2(\Phi) \leq d^{-1/2} \left( 1 + (d-1) \sup_{(j,k) \neq (0,0)} |\lambda_{jk}|^2 \right)^{1/2} \quad (42)$$

where  $\lambda_{jk}$  is given by (39). When  $d = 3$ , the bound is attained for a state of the form  $\frac{1}{3} [I + X^{j_*} Z^{k_*} + (X^{j_*} Z^{k_*})^2]$  where  $j_*, k_*$  denote the pair of integers for which the supremum is attained in (42).

**Proof:** Using the notation of (40),

$$\begin{aligned} \|\Phi(\rho)\|_2^2 &= \text{Tr} [\Phi(\rho)]^\dagger \Phi(\rho) \\ &= \frac{1}{d^2} \sum_{ikj\ell} \bar{\lambda}_{ik} \bar{w}_{ik} \lambda_{j\ell} w_{j\ell} \text{Tr } Z^{-k} X^{-i} X^j Z^\ell \\ &= \frac{1}{d} \sum_{jk} |\lambda_{jk}|^2 |w_{jk}|^2 \\ &\leq \frac{1}{d} \left[ 1 + \sup_{(j,k) \neq (0,0)} |\lambda_{jk}|^2 \sum_{(j,k) \neq (0,0)} |w_{jk}|^2 \right] \\ &= \frac{1}{d} \left[ 1 + (d-1) \sup_{(j,k) \neq (0,0)} |\lambda_{jk}|^2 \right] \end{aligned} \quad (43)$$



with  $\lambda_{jk}$  given by (39). One can then verify that the bound is attained with the indicated state. **QED**

Fukuda and Holevo [8] independently proved the inequality (42). Moreover, when equality holds for some channel  $\Phi_1$ , then the multiplicativity conjecture (16) holds for  $p = 2$  with  $\Phi_2$  any other CPT map. In Example 3, we show that that equality holds for a special class of Pauli diagonal channels.

### 4.3 Representations of density matrices

Since  $\mathcal{T}$  is an orthonormal basis for  $M_d$ , any density matrix can be written as

$$\rho = \frac{1}{d} \left[ I + \sum_{m=1}^{d^2-1} v_m T_m \right], \quad (44)$$

with  $v_m = \text{Tr } T_m^\dagger \rho$ . This implies  $|v_m| \leq \|T_m\| \text{Tr } \rho = 1$ . However, finding conditions on  $v_m$  which ensure that an expression of the form (44) is positive semi-definite is

far from trivial. When  $\rho$  is a pure state,  $1 = \text{Tr } \rho^2 = \frac{1}{d^2} \left[ 1 + \sum_{m=1}^{d^2-1} |v_m|^2 \right]$ , so that

$$\sum_{m=1}^{d^2-1} |v_m|^2 = d - 1. \quad (45)$$

Combining this with  $|v_m| \leq 1$  implies that every pure state has at least  $d$  non-zero coefficients (including  $v_0 = 1$ ). For mixed states, one can have fewer non-zero coefficients. For example, when  $d = 4$ ,  $\rho = \frac{1}{4}[I + Z^2]$ .

For  $\rho = |\psi\rangle\langle\psi|$  a pure state written in the form (44), define  $\mathcal{S}$  as the subgroup generated by  $\{T_m : v_m \neq 0\}$ . It follows from the fact that at least  $d$  coefficients are non-zero that any subgroups generated by a pure state in this way have  $|\mathcal{S}| \geq d$ .

In the generalized Pauli basis, two examples of  $\mathcal{S}$  are  $\{I, X, X^2, \dots, X^{d-1}\}$  and  $\{I, Z, Z^2, \dots, Z^{d-1}\}$ . In fact, any choice of  $W = X^j Z^k$  with  $j$  or  $k$  relatively prime to  $d$  generates a cyclic subgroup

$$\mathcal{S} = \{I, X^j Z^k, (X^j Z^k)^2, \dots, (X^j Z^k)^{d-1}\}, \quad (46)$$

and the projections onto orthogonal eigenvectors of  $W = X^j Z^k$  can be written as

$$|\psi_n\rangle\langle\psi_n| = \frac{1}{d} \left[ I + \sum_{j=0}^{d-1} \omega^{nj} W^j \right] \quad n = 1, 2, \dots, d \quad (47)$$

with  $\omega = e^{2\pi i/d}$ . We will call such states *axis states*. When  $d$  is prime, there are  $d + 1$  distinct subgroups of the form (46), whose eigenvectors generate  $d + 1$  orthogonal bases for  $\mathbf{C}^d$ . These are the  $d + 1$  mutually unbiased bases.

**Example 1** When  $d = 4$ ,  $\mathcal{S} = \{I, X^2, Z^2, X^2 Z^2\}$ . In this case, the elements of  $\mathcal{S}$  do not commute (although the group is formally abelian) and do not have simultaneous eigenvectors. However,  $|\psi\rangle = (1, 0, 1, 0)$  satisfies

$$|\psi\rangle\langle\psi| = \frac{1}{4}[I + Z^2 + X^2 + X^2 Z^2] \quad (48)$$

and  $N^{C,T}(|\psi\rangle\langle\psi|)$  is decomposable.

**Example 2** When  $d = 4$ ,  $\mathcal{S} = \{I, Z^2, X, XZ^2, X^2, X^2 Z^2, X^3, X^3 Z^2\}$ . is another subgroup, which has order  $2d$ . For  $|\psi\rangle = (a, b, a, b)$

$$|\psi\rangle\langle\psi| = \frac{1}{2}[(a^2 + b^2)(I + X^2) + (a^2 - b^2)Z^2(I + X^2)X^2 Z^2 + 2abX(I + X^2)]. \quad (49)$$

Note that this pure state does not require the full subgroup, i.e., the coefficients of  $XZ^2$  and  $X^3 Z^2$  are zero. (This can not happen for subgroups of order  $d$ .) The terms  $XZ^2$  and  $X^3 Z^2$  do arise in the product  $\rho^2$ , but since  $ab(XZ^2 + Z^2 X) = ab(XZ^2 - XZ^2) = 0$  the coefficients are zero.

**Example 3** Let  $W_L(\nu = 1, 2 \dots d+1)$  denote a set of fixed generators for  $\kappa$  cyclic groups of the form (46), chosen so that the groups are mutually disjoint except for the identity. Let

$$\Omega = s\mathcal{I} + \sum_{L=1}^{\kappa} t_L \Psi_L^{\text{QC}} + u\mathcal{N} \quad (50)$$

where  $\Psi_L^{\text{QC}}$  is the channel that maps a state  $\rho$  onto its diagonal when it is written in the axis basis (44) for  $W_L$ . The condition  $s + \sum_L t_L + u = 1$  implies that  $\Omega$  is trace-preserving, and the conditions

$$a_0 = s + \frac{1}{d} \sum_L t_L + \frac{1}{d^2} u \geq 0, \quad a_L \equiv \frac{1}{d} t_L + \frac{1}{d^2} u \geq 0 \quad (51)$$

are necessary and sufficient for  $\Omega$  to be CP. With the correspondence  $T_m \sim X^j Z^k \sim W_L^n$ , the coefficients in (32) depend only on  $L$  and are given by (51). Moreover, the parameters in (39) also depend only on  $L$  and satisfy  $\lambda_{jk} \sim \lambda_L = s + t_L$ . Let  $\lambda \equiv \max_L |\lambda_L| \equiv \max_L |s + t_L|$ . One can verify that  $[\nu_2(\Omega)]^2 = \frac{1}{d}[1 + (d-1)\lambda^2]$  is attained with the axis states (47) for an  $L$  which attains  $\lambda$ . Thus, by Theorem 2 in [8], multiplicativity (16) holds for  $\Omega \otimes \Phi$  when  $p = 2$  and  $\Phi$  is any CPT map. The case of only one non-zero  $t_L$  was also considered in [8]. Extensions to mutually unbiased bases when  $d$  is a prime power are considered in [32].

## 4.4 Image of the completely noisy conjugate

The coefficients  $v_m$  form the first row of the matrix  $N^{C,T}(\rho)$  so that  $\rho \neq \gamma$  implies  $N^{C,T}(\rho) \neq N^{C,T}(\gamma)$ . This uniqueness allows one to consider  $N^{C,T}(\rho)$  as a representation of the set of density matrices, and (44) might be regarded as a generalization of the Bloch sphere representation. Indeed, if the (non-unitary standard basis) is ordered so that  $T_{j+(k-1)d} = E_{jk} = |j\rangle\langle k|$ , then  $N^{C,T}(\rho) = \frac{1}{d}I_d \otimes \rho$ . Combining this observation with Lemma 1 gives

**Theorem 10** *For any basis  $\mathcal{T}$  satisfying (30), there is a unitary matrix  $U_{\mathcal{T}}$  such that  $N^{C,T}(\rho) = U_{\mathcal{T}} \frac{1}{d}I_d \otimes \rho U_{\mathcal{T}}^\dagger$ .*

This result has an interesting interpretation with potential applications. It says, in the terminology of the introduction, that one can actually use noise to transmit information for Alice to Bob. In fact, when the noise has completely destroyed Alice's information (i.e., her density matrix is  $\frac{1}{d}I$ ), Bob has a faithful copy. This may be counter-intuitive because his density matrix also has entropy at least  $\log d$ . However, Bob's system has dimension  $d^2$  and can be regarded as itself a composite of two  $d$ -dimensional subsystems  $B_1$  and  $B_2$ . Theorem 10 implies that Bob can make a unitary transformation on his system so that all the noise is in one room and a faithful copy of Alice's original quantum state in the other. Note that this result applies to mixed, as well as pure, inputs.

Combining Theorem 10 with (33) gives the following

**Corollary 11** *The conjugate of a Pauli diagonal channel can be written as*

$$\Phi^{C,P}(\rho) = \sqrt{A} U_{\mathcal{P}} \frac{1}{d} I_d \otimes \rho U_{\mathcal{P}}^\dagger \sqrt{A} = F I_d \otimes \rho F^\dagger \quad (52)$$

where,  $U_{\mathcal{P}}$  is the unitary matrix which transforms the standard basis  $\{E_{jk}\}$  to the generalized Pauli basis,  $A$  is a positive diagonal operator with  $\text{Tr } A = 1$ , and  $F = d^{-1/2} \sqrt{A} U_{\mathcal{P}}$ .

This is essentially the Stinespring representation for  $\Phi^{C,P}(\rho)$ . Since  $\Phi^{C,P}(\rho)$  is trace-preserving,  $\text{Tr}_1 F^\dagger F = \text{Tr}_1 \frac{1}{d} U_{\mathcal{P}}^\dagger A U_{\mathcal{P}} = I_2$ . A similar result holds for other channels which are diagonal with respect to a set of unitary Kraus operators.

**Theorem 12** *For any pure state  $|\psi\rangle\langle\psi|$ , the state  $N^C(|\psi\rangle\langle\psi|)$  satisfies the following conditions:*

- a)  $d N^{C,T}(|\psi\rangle\langle\psi|)$  is a projection of rank  $d$ , and

b) all diagonal elements of  $N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)$  equal  $\frac{1}{d^2}$ .

In addition, if  $T_m$  satisfies (35) then

c) all elements of  $N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)$  are  $\leq \frac{1}{d^2}$ , and

d)  $d^3 N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|) * \overline{N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)}$  is a double stochastic matrix.

Theorem 12 provides a set of necessary conditions for a matrix in  $M_{d^2}$  to be  $N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)$  for some pure state. However, there are matrices in  $M_{d^2}$  which satisfy (a), (b), (c), (d) above, but can *not* be realized as the image  $N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)$  of any pure state density matrix.

A particularly interesting subset of  $\mathcal{N}$  consists of those for which exactly  $d$  of the  $w_m$  have  $|w_m| = 1$  and the rest are zero. When the operators (36) are used,  $N^C(\rho)$  is permutationally equivalent to a block diagonal matrix with  $d \times d$  blocks on the diagonal, each of which is rank one and has all elements with magnitude 1. We will call such  $N^C(\rho)$  *d-decomposable*. (In general, a decomposable matrix is one which is permutationally equivalent to a block diagonal matrix). Theorem 12 implies that all decomposable matrices in  $\mathcal{N}^{\mathcal{T}}$  have blocks of the same size.

Let  $\mathcal{S}$  be the subgroup of  $\mathcal{T}$  associated with a pure state as in Section 4.3, or, equivalently, generated by the non-zero elements of the first row of  $N^{C,\mathcal{T}}(|\psi\rangle\langle\psi|)$ . The cosets  $T_k\mathcal{S}$  define a partition of the integers  $\{0, 1, \dots, d^2 - 1\}$ . Moreover, if  $T_m$  satisfy (35), and  $|\mathcal{S}| < d$ , then  $N^{C,\mathcal{T}}(\rho)$  is decomposable and the decomposition into blocks corresponds to the partition determined by the cosets of  $\mathcal{S}$ . When the order of  $\mathcal{S}$  is  $d$ , it follows from Theorem 12 that each block is a rank 1 projection with diagonal elements  $\frac{1}{d}$ ; this implies that all of the non-zero coefficients satisfy  $|v_m| = 1$ .

**Theorem 13** *Let  $d$  be prime and  $\mathcal{P} \otimes \mathcal{P}$  the basis for  $M_{d^2}$  consisting of tensor products of generalized Pauli matrices. If  $N^{C,\mathcal{P} \otimes \mathcal{P}}(|\psi\rangle\langle\psi|)$  is  $d^2$ -decomposable, then  $|\psi\rangle$  is either a product state or a maximally entangled state.*

**Proof:** First observe that for an arbitrary  $|\psi\rangle \in \mathbf{C}^{d^2} \simeq \mathbf{C}^d \otimes \mathbf{C}^d$

$$|\psi\rangle\langle\psi| = \frac{1}{d^2} \sum_{mn} c_{mn} T_m \otimes T_n. \quad (53)$$

When  $N^{C,\mathcal{P} \otimes \mathcal{P}}(|\psi\rangle\langle\psi|)$  is  $d^2$ -decomposable, at most  $d^2$  of the  $d^4$  coefficients  $c_{mn}$  are non-zero, and the corresponding  $T_m \otimes T_n$  generate a subgroup of order at most  $d^2$ .

This implies that (53) must reduce to one of the following two forms.

$$\gamma_{12} = |\psi_{12}\rangle\langle\psi_{12}| = \frac{1}{d^2} \left( I \otimes I + \sum_{m=1}^{d^2-1} e^{i\theta_m} T_m \otimes T_{\pi(m)} \right) \quad (54)$$

where  $\pi$  is a permutation of  $\{1, 2 \dots d^2 - 1\}$ , or,

$$\gamma_{12} = |\psi_{12}\rangle\langle\psi_{12}| = \frac{1}{d^2} \sum_{m=0}^{d^2-1} \sum_{n=0}^{d^2-1} e^{i\theta_{mn}} V^m \otimes W^n \quad (55)$$

where  $V = X^i Z^k$  for some fixed  $i, k$  and  $W = X^j Z^\ell$  for some fixed  $j, \ell$ .

In the first case (54) we have used the fact that the trace-preserving property requires the term  $I \otimes I$  and the requirement of a group of order  $d^2$  implies that once one goes beyond a cyclic subgroup each  $T_m$  can only occur once. In this case, it is immediate that  $\gamma_1 = \gamma_2 = \frac{1}{d} I$  which implies that  $\psi_{12}$  is maximally entangled.

In the second case (55), the subgroup is a direct product of cyclic subgroups. The requirement that  $|\psi_{12}\rangle$  is pure is equivalent to

$$e^{i\theta_{mn}} = \frac{1}{d^2} \sum_s \sum_t e^{i\theta_{st}} e^{i\theta_{m-s, n-t}} \quad (56)$$

with subscript addition mod  $d$ . It then follows from the triangle inequality that

$$1 \leq \frac{1}{d^2} \sum_{st} 1 = 1, \quad (57)$$

which implies  $e^{i\theta_{m-s, n-t}} = e^{i\theta_{mn}} e^{-i\theta_{st}}$

Now, since  $\text{Tr } V^m = d\delta_{m0}$ ,  $\gamma_1 = \text{Tr } \gamma_{12} = \frac{1}{d} \sum_m e^{i\theta_{m0}} V^m$ , and the condition that  $\gamma_1$  is pure is  $e^{i\theta_{m0}} = \frac{1}{d} \sum_s e^{i\theta_{s0}} e^{i\theta_{m-s, 0}}$ . But this holds, since we have already shown that  $e^{i\theta_{m-s, 0}} = e^{i\theta_{m0}} e^{-i\theta_{s0}}$ . Therefore,  $\rho_1$  is a pure state  $|\psi_1\rangle\langle\psi_1|$ ; similarly  $\rho_2 = |\psi_2\rangle\langle\psi_2|$ . Since  $\rho_{12}$  is pure, this implies that  $|\psi_{12}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$  is a product. **QED**

We conclude this section with an explicit expression for  $N^{C,T}(|\psi\rangle\langle\psi|)$  in the generalized Pauli basis.

**Theorem 14** *In the generalized Pauli basis,*

$$N^{C,\mathcal{P}}(|\psi\rangle\langle\psi|) = \sum_{\ell} X^\ell R |\psi\rangle\langle\psi| R X^{-\ell} \otimes Z^\ell |\iota\rangle\langle\iota| Z^{-\ell} \quad (58)$$

where  $|\iota\rangle$  is the vector whose elements are all 1 and  $R \sum_k v_k |k\rangle = \sum_k v_{d-k} |k\rangle$ , i.e.,  $R$  reverses the order of the elements of a vector.

As an immediate corollary, we find that

$$\mathcal{N}^{C,\mathcal{P}} = \left\{ \sum_{\ell} X^{\ell} |\psi\rangle\langle\psi| X^{-\ell} \otimes Z^{\ell} |\iota\rangle\langle\iota| Z^{-\ell} : \psi \in \mathbf{C}^d \right\} \quad (59)$$

**Proof:** By a straightforward calculation one finds

$$\begin{aligned} N^{C,\mathcal{P}}(|\psi\rangle\langle\psi|) &= \sum_{jk} \sum_{mn} |j \otimes m\rangle\langle k \otimes n| \text{Tr } X^j Z^m |\psi\rangle\langle\psi| (X^k Z^n)^{\dagger} \\ &= \sum_{jk} \sum_{mn} \sum_{\ell} \bar{\psi}_{\ell} \psi_{\ell} \omega^{(m-n)\ell} \langle \ell + j, \ell + k \rangle |j \otimes m\rangle\langle k \otimes n| \\ &= \sum_{\ell} \left( \sum_{jk} \bar{\psi}_{\ell-j} \psi_{\ell-k} |j\rangle\langle k| \right) \otimes \left( \sum_{mn} |m\rangle\langle n| \right) \omega^{(m-n)\ell} \end{aligned}$$

where  $\omega = e^{2\pi i/d}$ .

**QED**

Note that the last line says that each block of  $N^{C,\mathcal{P}}(|\psi\rangle\langle\psi|)$  is cyclic, and the expression is consistent with the fact that the first row determines the rest.

## 4.5 Upper bound on $\nu_p(\Phi)$

**Theorem 15** *For a channel of the form (32), let  $b_j$  be a rearrangement of  $a_j$  in non-increasing order, and define  $\beta_j = \sum_{i=0}^{d-1} b_{i+jd}$ ,  $0 \leq j \leq d-1$ . Then*

$$\nu_p(\Phi) = \nu_p(\Phi^{C,\mathcal{T}}) \leq \left( \sum_{i=0}^{d-1} \beta_i^p \right)^{1/p} \quad (60)$$

Moreover, if equality holds,  $\Phi^{C,\mathcal{T}}(\rho)$  is decomposable for a  $\rho$  that maximizes the  $p$ -norm.

**Proof:** By (34), it suffices to bound  $\|\gamma A \gamma\|_p$  for  $\gamma \in \mathcal{N}^{\mathcal{T}}$ . Every eigenvector of  $\gamma A \gamma$  corresponding to a non-zero eigenvalue is in the range of  $\gamma$ . Therefore, we can choose an orthonormal basis for the range of  $\gamma$  consisting of normalized eigenvectors  $|f_i\rangle$  of  $\gamma A \gamma$  arranged in order of non-increasing eigenvalues  $\lambda_i$ . (It may be necessary to include some eigenvectors with eigenvalue zero.) By Theorem 12,  $d\gamma$  is projection of rank  $d$ ; therefore, we can write

$$\gamma = \frac{1}{d} \sum_{i=0}^{d-1} |f_i\rangle\langle f_i|. \quad (61)$$

Since  $A$  is diagonal with elements  $a_r \delta_{rs}$  in the standard basis  $\{|e_r\rangle\}$ , we find

$$\lambda_i = \langle f_i | \gamma A \gamma | f_i \rangle = \frac{1}{d^2} \langle f_i | A | f_i \rangle = \frac{1}{d^2} \sum_{r=0}^{d^2-1} a_r |\langle f_i | e_r \rangle|^2 \quad (62)$$

for  $i = 1 \dots d$ . The inequality (60) will follow from standard results [15, 27] if we can show that the eigenvalues of  $d^3 \gamma A \gamma$  are majorized by  $\{\beta_i\}$ .

By part (b) of Theorem 12 ,

$$\sum_i |\langle f_i | e_r \rangle|^2 = d \langle e_r | \gamma | e_r \rangle = \frac{1}{d}. \quad (63)$$

Since  $|f_i\rangle$  is a unit vector, we also have  $\sum_r |\langle f_i | e_r \rangle|^2 = 1$ . Therefore

$$\sum_{i=0}^{k-1} \sum_{r=0}^{d^2-1} |\langle f_i | e_r \rangle|^2 = k = \sum_{i=0}^{d-1} \sum_{r=0}^{kd-1} |\langle f_i | e_r \rangle|^2. \quad (64)$$

Removing the common terms  $\sum_{i=0}^{k-1} \sum_{r=0}^{kd-1} |\langle f_i | e_r \rangle|^2$  in (64) gives the identity

$$\sum_{i=0}^{k-1} \sum_{r=kd}^{d^2-1} |\langle f_i | e_r \rangle|^2 = \sum_{i=k}^{d-1} \sum_{r=0}^{kd-1} |\langle f_i | e_r \rangle|^2. \quad (65)$$

Since  $b_r$  is a rearrangement of  $a_r$ , we can assume without loss of generality that the basis  $|e_r\rangle$  has been chosen to correspond to the ordering of  $b_r$ . Then  $s < kd < t$  implies  $b_s \geq b_{kd} \geq b_t$  and it follows that for each  $k = 1, 2, \dots, d-1$ .

$$d^3 \sum_{i=0}^{k-1} \lambda_i = d \sum_{i=0}^{k-1} \sum_{r=0}^{d^2-1} b_r |\langle f_i | e_r \rangle|^2 \quad (66)$$

$$\begin{aligned} &= d \sum_{r=0}^{kd-1} b_r \left( \sum_{i=0}^{k-1} |\langle f_i | e_r \rangle|^2 \right) + d \sum_{r=kd}^{d^2-1} b_r \left( \sum_{i=0}^{k-1} |\langle f_i | e_r \rangle|^2 \right) \\ &\leq d \sum_{r=0}^{kd-1} b_r \left( \sum_{i=0}^{k-1} |\langle f_i | e_r \rangle|^2 \right) + d b_{kd} \sum_{i=k}^{d-1} \sum_{r=0}^{kd-1} |\langle f_i | e_r \rangle|^2 \\ &\leq d \sum_{r=0}^{kd-1} b_r \left( \sum_{i=0}^{d-1} |\langle f_i | e_r \rangle|^2 \right) \\ &\leq \sum_{r=0}^{kd-1} b_r = \sum_{j=0}^{k-1} \beta_j \end{aligned} \quad (67)$$

where we used (65) for the first inequality. For  $k = d$ , it follows immediately from (63) and (66) that

$$d^3 \sum_{i=0}^d \lambda_i = \sum_{r=0}^{d^2-1} b_r = \sum_{j=0}^d \beta_j$$

Thus, the eigenvalues of  $d^3 \gamma A \gamma$  are majorized  $\{\beta_i\}$ . If  $\gamma$  is not decomposable, then for some  $r$ ,

$$0 < |\langle f_1 | e_r \rangle|^2 < \sum_{i=0}^{d-1} |\langle f_i | e_r \rangle|^2 = \frac{1}{d^2} \quad (68)$$

which implies a strict inequality in (67).

**QED**

Note that the numbers  $\beta_j$  define a partition of the integers  $\{0, 1, \dots, d^2 - 1\}$ . Let  $0, m_1, m_2, \dots, m_{d-1}$  be the subset which contains 0, and let

$$\mathcal{S} = \{I, T_{m_1}, T_{m_2}, \dots, T_{m_{d-1}}\}. \quad (69)$$

If the set  $\mathcal{S}$  is not a subgroup of  $\mathcal{T}$  then there is no pure state  $\rho$  which will generate a  $d$ -decomposable  $\gamma \in \mathcal{N}^{\mathcal{T}}$  for which the upper bound (60) is attained.

## 4.6 Applications to Multiplicativity

To use Theorem 15 to prove multiplicativity (16), one would need to show that the upper bound (60) is attained for both  $\Phi$  and  $\Phi \otimes \Phi$ . Unfortunately, this is almost never true for  $\Phi \otimes \Phi$ , and for the few exceptions multiplicativity is well-known and easily proved. One can, however, prove a new result for the  $p = \infty$  norm. Before doing so, we present two insightful examples.

When a channel has the form (32) in the generalized Pauli basis, we use slight abuse of notation and write  $a_{jk}$  for the weight given to conjugations with  $X^j Z^k$ .

**Example 4** *QC channels:* If  $a_{jk} = a_j$  does not depend on  $k$ , then  $\beta_j = da_j$  and it is easy to see that the upper bound (60) can be attained and the corresponding channel is multiplicative in the sense

$$\nu_p(\Phi^{\otimes m}) = [\nu_p(\Phi)]^m \quad \forall p \geq 1 \quad \text{and} \quad \forall \text{ integers } m. \quad (70)$$

However, this does not lead to a new result because

$$\sum_{jk} a_j X^j Z^k \rho (X^j Z^k)^\dagger = \sum_j a_j X^j \left( \sum_k Z^k \rho Z^{-k} \right) X^{-j} = \sum_j a_j X^j \rho_{\text{diag}} X^{-j}. \quad (71)$$



The map  $\rho \mapsto \rho_{\text{diag}}$  is a special type of EBT channel called quantum-classical (QC). Therefore, (71) is an EBT map.

**Example 5** The depolarizing channel is defined as

$$\Phi(\rho) = b\rho + \frac{1-b}{d}\text{Tr } \rho I, \quad (72)$$

For this channel,  $\nu_p(\Phi)$  is easily computed and known to satisfy  $\nu_p(\Phi \otimes \Phi) = [\nu_p(\Phi)]^2$ . When  $b > 0$ ,  $\Phi$  can be written in the form (32) with  $a_0 > a_j$  and  $a_j = \frac{1-a_0}{d^2-1} = (1-b)\frac{1}{d^2}$  for  $j \geq 1$ . The upper bound can be attained with a decomposable state. However, the tensor product  $\Phi \otimes \Phi$  does *not* attain the upper bound in the basis given by tensor products of generalized Pauli matrices. To see why, observe that in this product basis  $\beta_0 = a_0^2 + (d^2-1)a_0a$ . But it is known [8, 19] that this channel is multiplicative for all  $p$ , which implies that its largest eigenvalue is  $[b + \frac{1-b}{d}]^2 = [a_0 + (d-1)a]^2$ . Since

$$[a_0 + (d-1)a]^2 = a_0^2 + 2(d-1)a_0a + (d-1)^2a^2 < a_0^2 + (d^2-1)a_0a = \beta_0$$

the upper bound is not attained. Although the product density matrix which attains  $[\nu_p(\Phi)]^2$  can be chosen to be decomposable, its blocks do not correspond to a partition which attains the upper bound.

When  $-\frac{1}{d} \leq b < 0$ , one has  $a_0 < a_j$  for  $j \geq 1$ , but a similar analysis shows that the upper bound is not attained for  $\Phi \otimes \Phi$ .

The problems which arise in the depolarizing channel are generic. This is most easily seen by examining the qubit case in detail, which is done in Appendix B. The most one can hope to obtain is the following result for the infinity norm.

**Theorem 16** *Let  $\Phi$  be a Pauli diagonal channel and  $b_{jk}$  a rearrangement of  $a_{jk}$  as in Theorem 15 so that  $\beta_j = \sum_k b_{jk}$ . Let  $j_*$  denote the index for which  $a_{00} = b_{j_*k}$  for some  $k$ , and*

$$\mathcal{S} = \{X^m Z^n : a_{mn} = b_{j_*k}, k = 0, 1, \dots, d-1\}. \quad (73)$$

*Then the upper bound (60) is attained if and only if  $\mathcal{S}$  is a subgroup of  $\mathcal{T}$  and its partition into cosets corresponds to the partition defined by the  $\beta_j$ , i.e., each coset has the form*

$$T_\ell \mathcal{S} = \{X^m Z^n : a_{mn} = b_{jk}, k = 0, 1, \dots, d-1\} \quad \text{for some } j.$$

If, moreover,  $b_{0,d-1}^2 > b_{00} b_{10}$  (under the assumption  $b_{jk} \geq b_{j,k+1}$ ), then

$$\nu_\infty(\Phi \otimes \Phi) = [\nu_\infty(\Phi)]^2. \quad (74)$$

More generally, if  $b_{0,d-1}^r > b_{00}^{r-1} b_{10}$ , then  $\nu_\infty(\Phi^{\otimes r}) = [\nu_\infty(\Phi)]^r$ .

**Proof:** The first part is essentially a matter of notation and our earlier discussion about subgroups and partitions. For the second part, it suffices to observe that the inequality implies that the largest  $\beta$  for  $\Phi \otimes \Phi$  is  $\beta_0^2$ . **QED**

## 5 Giovannetti-Lloyd linearization operators

In [9] a linearization of  $p$ -norm functions was introduced and subsequently used [10, 11] used to prove multiplicativity for integer  $p$  and certain special types of channels. For any integer  $p$ , it is possible to find a linear operator  $X(\Phi, p)$  in  $\mathcal{H}^{\otimes p}$  such that

$$\text{Tr}(\Phi(\rho))^p = \text{Tr}(\rho^{\otimes p} X(\Phi, p)) \quad (75)$$

holds for any  $\rho$ .  $X(\Phi, p)$  is not uniquely defined. Initially [9, 10], the realization  $\Theta(\Phi, p)$ , defined in terms of the Kraus operators  $A_k$  of  $\Phi$  as

$$\Theta(\Phi, p) = \sum_{k_1, \dots, k_p} A_{k_1}^\dagger A_{k_2} \otimes A_{k_2}^\dagger A_{k_3} \otimes \dots \otimes A_{k_p}^\dagger A_{k_1} \quad (76)$$

was used. However, (76) satisfies (75) only when the input is a pure state. In [11], the operator

$$\Omega(\Phi, p) \equiv \widehat{\Phi}^{\otimes p}(L_p) \quad (77)$$

was introduced where  $\widehat{\Phi}$  denotes the adjoint with respect to the Hilbert-Schmidt inner product and  $L_p$  and  $R_p$  are the left shift and the right shift operators

$$\begin{aligned} L_p |k_1 k_2 \dots k_p\rangle &= |k_2 \dots k_p k_1\rangle, \\ R_p |k_1 \dots k_{p-1} k_p\rangle &= |k_p k_1 \dots k_{p-1}\rangle, \end{aligned}$$

$\Omega(\Phi, p)$  was shown to give a valid realization of  $X$  for arbitrary  $\rho$  and satisfy

$$\Omega(\Phi, p) = \Theta(\Phi, p) L_p \quad (78)$$

We now give some relations between these operators and those of their conjugates.

**Theorem 17** *Let  $\Phi$  be a CPT map and let  $\Theta(\Phi, p)$  and  $\Omega(\Phi, p)$  be the linearizing operators defined above using a fixed set of Kraus operators. Then*

$$\Omega(\Phi, p) = \Theta(\Phi^C, p)^\dagger = \Theta(\Phi, p)L_p. \quad (79)$$

when  $\Phi^C$  is defined using the Kraus representation given by (8).

**Proof:** The key point is that (8) implies that conjugate sets of Kraus operators satisfy

$$\langle m|F_\mu = \sum_j \langle j|(F_\mu)_{mj} = \sum_j \langle j|(F_m)_{\mu j} = \langle m|R_m. \quad (80)$$

Then

$$\begin{aligned} \Omega(\Phi, p) &= \widehat{\Phi}^{\otimes p}(L_p) = \widehat{\Phi}^{\otimes p}\left(\sum_{k_1, \dots, k_p} |k_2 \cdots k_p k_1\rangle \langle k_1 k_2 \cdots k_p|\right) \\ &= \sum_{k_1, \dots, k_p} \widehat{\Phi}(|k_2\rangle \langle k_1|) \widehat{\Phi}(|k_3\rangle \langle k_2|) \otimes \cdots \otimes \widehat{\Phi}(|k_1\rangle \langle k_p|) \\ &= \sum_{k_1, \dots, k_p} \sum_{\mu_1, \dots, \mu_p} F_{\mu_1}^\dagger |k_2\rangle \langle k_1| F_{\mu_1} \otimes F_{\mu_2}^\dagger |k_3\rangle \langle k_2| F_{\mu_2} \otimes \cdots \otimes F_{\mu_p}^\dagger |k_1\rangle \langle k_p| F_{\mu_p} \\ &= \sum_{k_1, \dots, k_p} \sum_{\mu_1, \dots, \mu_p} R_{k_2}^\dagger |\mu_1\rangle \langle \mu_1| R_{k_1} \otimes R_{k_3}^\dagger |\mu_2\rangle \langle \mu_2| R_{k_2} \otimes \cdots \otimes R_{k_1}^\dagger |\mu_p\rangle \langle \mu_p| R_{k_p} \\ &= \sum_{k_1, \dots, k_p} R_{k_2}^\dagger R_{k_1} \otimes R_{k_3}^\dagger R_{k_2} \otimes \cdots \otimes R_{k_1}^\dagger R_{k_p}. \quad \text{QED} \end{aligned} \quad (81)$$

Theorem 17 allows one to compute  $\Omega(\Phi, p)$  from the Kraus operators of  $\Phi^C$  without using shift operators. Conversely, one can compute  $\Theta(\Phi, p) = \Omega(\Phi^C, p)$  directly in terms of the action of  $\Phi^C$  on components of shift operators, without knowing its Kraus expansion or requiring a final multiplication by a shift operator.

**Acknowledgements:** The work of CK and MN was supported in part by National Science Foundation Grant DMS-0400426. The work of KM was partially supported by the ERATO Quantum Computation and Information Project of the Japan Science and Technology Agency. The work of MBR and MN was partially supported by the National Science Foundation under Grant DMS-0314228 and by the National Security Agency and Advanced Research and Development Activity under Army Research Office contract number DAAD19-02-1-0065. This work is an outgrowth of discussions between MBR and KM during the program on Quantum Information at the Isaac Newton Institute at Cambridge University in 2004. Some

of the work of MBR was performed during a visit to the ERATO Quantum Computation and Information Project and National Institute of Informatics in Tokyo. Some of the work of MN was performed at Northeastern University.

## A Representations of CPT maps

We review here some facts about representations of CPT maps on finite dimensional spaces. For proofs and additional details about the history we recommend Chapter 4 of Paulsen [29].

In more general situations, a CPT map is defined as the dual of a unital CP map and some theorems are more conveniently stated for unital maps. In finite dimensions, a linear map  $\Phi : M_d \mapsto M_{d'}$  is trace-preserving if and only if its dual  $\widehat{\Phi} : M_{d'} \mapsto M_d$  is unital, where

$$\mathrm{Tr} [\widehat{\Phi}(A)]^\dagger B = \mathrm{Tr} A^\dagger \Phi(B), \quad (82)$$

Here, we will state results for unital maps in terms of  $\widehat{\Phi}$ .

The first and most fundamental result is due to Stinespring [35].

**Theorem 18** (Stinespring) *Let  $\Psi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{K})$  be a CP map from the  $C^*$ -algebra  $\mathcal{A}$  to the bounded operators on the Hilbert space  $\mathcal{K}$ . There exists a  $*$ -homomorphism  $\pi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$  from  $\mathcal{A}$  to the bounded operators on the Hilbert space  $\mathcal{H}$  and a bounded operator  $V : \mathcal{H} \mapsto \mathcal{K}$  such that*

$$\Psi(A) = V^\dagger \pi(A) V. \quad (83)$$

Moreover,  $\Psi$  is unital if and only if  $V^\dagger V = I$ .

This result may seem strange to those familiar with the operator sum representation; it has the same form, but with only a single term. However, the sum is hidden in the representation which can contain multiple copies of  $\mathcal{A}$ . In fact, for  $\Psi = \widehat{\Phi}$  with  $\Phi$  a CPT map as above, one can show [29] that  $\pi(A) = A \otimes I_\kappa = \sum_k A \otimes |e_k\rangle\langle e_k|$  with  $\kappa \leq dd'$ . Then defining  $F_k = (I_d \otimes \langle e_k|)V$ , we can write  $V = \sum_k F_k \otimes |e_k\rangle$  and

$$\widehat{\Phi}(A) = V^\dagger A \otimes I_\kappa V = \sum_k F_k^\dagger A F_k \quad (84)$$

with  $\sum_k F_k^\dagger F_k = V^\dagger V = I_{d'}$ . This is equivalent to the usual Kraus-Choi operator sum representation since, for any  $A \in C^{d'}$ ,  $B \in C_d$ ,

$$\text{Tr } A^\dagger \Phi(B) = \text{Tr} \sum_k [F_k^\dagger A F_k]^\dagger B = \text{Tr } A^\dagger \left( \sum_k F_k B F_k^\dagger \right), \quad (85)$$

which implies  $\Phi(B) = \sum_k F_k B F_k^\dagger$ .

Moreover,

$$\begin{aligned} \text{Tr } A^\dagger \Phi(B) &= \text{Tr} (A \otimes I_\kappa)^\dagger V B V^\dagger \\ &= \text{Tr} (A \otimes I_\kappa)^\dagger \left( \sum_{jk} F_j B F_k^\dagger \otimes |e_j\rangle\langle e_k| \right) \\ &= \text{Tr} (A \otimes I_\kappa)^\dagger U B \otimes |e_1\rangle\langle e_1| U^\dagger \end{aligned} \quad (86)$$

where  $U = \sum_{jk} U_{jk} \otimes |e_j\rangle\langle e_k|$  with each  $U_{jk}$  a  $d \times d'$  matrix and  $U_{j1} = F_j$  or, equivalently, the first  $d'$  columns of  $U$  equal  $V$ . Since  $V^\dagger V = I$ , this implies that  $U$  can be chosen to be a partial isometry of rank  $d\kappa$  so that when  $d = d'$ ,  $U$  is a unitary extension of  $V$ . Thus we conclude that any CPT map can be represented in the form

$$\Phi(B) = \text{Tr}_2 U B \otimes |e_1\rangle\langle e_1| U^\dagger \quad (87)$$

with  $U$  a partial isometry. This is sometimes referred to as the ‘‘Stinespring dilation theorem’’, although (87) does not appear explicitly in [35]; Kretschmann and Werner [?] use the term ‘‘ancilla representation’’. As far as we are aware Lindblad [26] was the first to explicitly use a representation of the form (87) and we will refer to it as the Lindblad-Stinespring ancilla representation.

Next, we consider the Choi-Jamiolkowski (CJ) representation of a CP map

$$\Gamma = (I \otimes \Phi)(|\phi\rangle\langle\phi|) = \frac{1}{d} \sum_{jk} |e_j\rangle\langle e_k| \otimes \Phi(|e_j\rangle\langle e_k|) \quad (88)$$

where  $|e_i\rangle$  denotes the standard basis for  $\mathbf{C}^d$  and  $|\phi\rangle = d^{-1/2} \sum_k |e_k \otimes e_k\rangle$  a maximally entangled state. The condition that  $\Phi$  is also trace-preserving becomes  $\text{Tr}_A \Gamma = \frac{1}{d} I_d$ . Let  $z^\mu, \mu = 1 \dots \kappa$  denote the normalized eigenvectors of  $\Gamma$  with a non-zero eigenvalue. Then  $\Gamma = \sum_{\mu=1}^\kappa \lambda_\mu |z^\mu\rangle\langle z^\mu|$ . Moreover, the identification  $g_{mj}^\mu = \sqrt{d\lambda_\mu} z_{(d'-1)m+j}^\mu$ , gives a set of Kraus operators  $G^\mu$  for the channel, and

$$\Gamma = \frac{1}{d} \sum_{jm,kt} \sum_{\mu} g_{mj}^\mu \bar{g}_{nk}^\mu |e_j \otimes e'_m\rangle\langle e_k \otimes e'_n|. \quad (89)$$

where  $|e'_m\rangle$  is the standard orthonormal basis for  $C_{d'}$ . Note that  $\kappa$  is the minimal number of Kraus operators and (up to degeneracy of eigenvectors) this provides a canonical way of defining a set of Kraus operators and shows that the minimal number is no greater than  $dd'$ .

**Proof of Proposition 2:** We can regard  $\Gamma$  as a density matrix  $\Gamma_{AB}$  on the tensor product space  $\mathbf{C}_d \otimes \mathbf{C}_{d'}$  and obtain a purification

$$\begin{aligned}\Gamma_{ABC} &= \sum_{\mu, nu} |\Psi_\mu \otimes e''_m u\rangle \langle \Psi_L \otimes e''_n u| \\ &= \sum_{\mu, \nu} \sum_{mj, nk} g_{mj}^\mu \bar{g}_{nk}^\nu |e_j \otimes e'_m \otimes e''_\mu\rangle \langle e_k \otimes e'_n \otimes e''_L| \end{aligned} \quad (90)$$

with  $\Psi_\mu = \sum_{jm} g_{mj}^\mu |e_j \otimes e'_m\rangle$  and Then, taking the partial trace over  $\mathcal{H}_B$  gives

$$\Gamma_{AC} = \sum_{\mu, \nu} \sum_{jkm} g_{mj}^\mu \bar{g}_{mk}^\nu |e_j \otimes e''_\mu\rangle \langle e_k \otimes e''_L| \quad (91)$$

which has eigenvectors  $\sum_{j\mu} g_{mj}^\mu |e_j \otimes e''_\mu\rangle$ . Thus,  $f_{\mu j}^m = g_{mj}^\mu$ ,  $m = 1 \dots d'$  form a set of Kraus operators for  $\Phi^C$  and  $\Gamma_{AC}$  is the CJ matrix  $(I \otimes \Phi^C)(|\phi\rangle\langle\phi|)$ . **QED**

It is well-known (see [29], Proposition 4.2) that any two minimal representations in Stinespring's dilation theorem are unitarily equivalent. Indeed, this is the reason there is no loss of generality in assuming that  $\pi(A) = A \otimes I_\kappa$  in (84). Similarly, it is easy to show that any two minimal sets of Kraus operators are related by a unitary transformation. However, it is often useful to consider non-minimal sets, in which case, the unitary transformation may be replaced by a partial isometry. Since this situation may be less familiar, we make a precise statement.

**Theorem 19** *If  $\{G_k\}$  is a minimal set of Kraus operators for the CPT map  $\Phi$  and  $U$  is partial isometry with  $U^\dagger U = I_\kappa$ , then*

$$F_j = \sum_k u_{jk} G_k \quad (92)$$

*is also a set of Kraus operators. Moreover, any two sets of Kraus operators  $\{F_j\}$  and  $\{F'_j\}$  define the same CPT map if and only if one can find a partial isometry  $W$  of rank  $\kappa$  such that  $F_j = \sum_k w_{jk} F'_k$ .*

**Proof:** The first assertion is easy to verify. Moreover, any set of Kraus operators defines a set of vector of length  $dd'$  whose span is the range of the CJ matrix.

When one set  $G_K$  is minimal, as in (92), the requirement that  $\Phi$  is trace-preserving implies that  $U^\dagger U = I_\kappa$ . When both  $\{F_j\}$  and  $\{F'_j\}$  they must satisfy (92) with  $G_k$  minimal and  $U, U'$  partial isometries of rank  $\kappa$ . Then  $G_k = \sum_j \bar{u}_{jk} F_j$ . Therefore,  $F'_j = \sum_k \sum_m u'_{jk} \bar{u}_{mk} F_m$  and  $W = U' U^\dagger$  satisfies  $W W^\dagger = U' U^\dagger U (U')^\dagger = U' (U')^\dagger$ , which is a projection of rank  $\kappa$ . Although, we do not have  $W^\dagger W = I$ , reversing the roles of  $\{F_j\}$  and  $\{F'_j\}$  gives  $F'_j = \sum_k v_{jk} F_k$  with  $V = U (U')^\dagger = W^\dagger$ .

## B Qubit channels

In the case of qubits, the decomposable images have the form  $\frac{1}{2} N^C [I \pm \sigma_j]$  with  $j = 1, 2, 3$  and are permutationally equivalent to  $\frac{1}{4} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & \pm i \\ 0 & 0 & \mp i & 1 \end{pmatrix}$ .

A channel of the form (32) can be rewritten as  $\Phi(I + \mathbf{w} \cdot \sigma) = I + \sum_k \lambda_k w_k \sigma_k$  with  $\frac{1}{2}(1 + \lambda_k) = a_0 + a_k$  and  $\frac{1}{2}(1 - \lambda_k) = a_i + a_j$  (with  $i, j, k$  distinct). With  $k^*$  chosen so that  $|\lambda_{k^*}| \geq |\lambda_j| \forall j = 1, 2, 3$ , one finds

$$\begin{aligned} \nu_p(\Phi) &= \left( \left[ \frac{1}{2}(1 + \lambda_{k^*}) \right]^p + \left[ \frac{1}{2}(1 - \lambda_{k^*}) \right]^p \right)^{1/p} \\ &= \left[ (a_0 + a_{k^*})^p + (a_i + a_j)^p \right]^{1/p} \end{aligned} \quad (93)$$

where we used the convention that  $i, j, k^*$  are distinct. When  $\lambda_{k^*} > 0$ ,  $a_0$  and  $a_{k^*}$  are the two largest coefficients; when  $\lambda_{k^*} < 0$ , they are the two smallest. Thus, the bound (60) is attained with either of the two decomposable matrices  $\frac{1}{2} N^C (I \pm \sigma_{k^*})$ .

In general the upper bound (60) is *not* attained for the product  $\Phi \otimes \Phi$ . To simplify the discussion, we now assume that  $a_0 > a_1 > a_2 \geq a_3$  which implies  $1 > \lambda_1 > \lambda_2 \geq \lambda_3$  and  $\lambda_2 > 0$  and involves no fundamental loss of generality. (One can always conjugate with  $\sigma_{k^*}$  to make  $a_0$  the largest and rotate axes to make  $a_1$  the second largest.) King [18] showed that all unital qubit channels are multiplicative for all  $p \geq 1$ . Therefore the eigenvalues of the optimal output of  $\Phi \otimes \Phi$  are  $\beta_1^2, \beta_1 \beta_2, \beta_2 \beta_1, \beta_2^2$  with

$$\beta_1^2 = (a_0 + a_1)^2, \quad \beta_1 \beta_2 = (a_0 + a_1)(a_2 + a_3) = \beta_2 \beta_1, \quad \beta_2^2 = (a_2 + a_3)^2.$$

The first term in the upper bound equals  $\beta_1^2$ , if and only if  $a_1^2 \geq a_0 a_2$ . Then the ordering of the product coefficients begins

$$a_0^2 > a_0 a_1 = a_1 a_0 > a_1^2 > a_0 a_2 = a_2 a_0 \dots$$

so that the second term in the upper bound is either  $2a_0(a_2 + a_3)$  or  $2(a_0 + a_1)a_2$ , neither of which equals  $\beta_1\beta_2$ . Thus, the upper bound (60) is never attained with distinct  $a_k$ . It is achieved if  $a_0 = a_1$  and  $a_2 = a_3$ , but this is a QC channel.

Although the multiplicativity of unital qubit channels was established in [18], it would be desirable to prove this by the methods developed here. This requires two additional assumptions

- a) The state in  $\mathcal{N}^{\mathcal{T}}$  which achieves  $\nu_p(\Phi \otimes \Phi)$  for a unital qubit channel  $\Phi$  is decomposable when  $\mathcal{T} = \mathcal{P} \otimes \mathcal{P}$  is the product Pauli basis.
- b) When  $d = 4$  and  $\mathcal{T}$  is the product Pauli basis, all decomposable states in  $\mathcal{N}^{\mathcal{P} \otimes \mathcal{P}}$  are either tensor products of axis states for  $d = 2$  or maximally entangled states formed from evenly weighted superpositions of axis states.

Although (a) seems like a reasonable conjecture, we have no proof. Theorem 13 implies (b); for qubits, an explicit computation can show that these maximally entangled states must have the form of the usual Bell states in one of the three axis bases. Then a direct comparison of the short list of possible decomposable states shows that  $\|\gamma A \gamma\|_p$  is always less for the maximally entangled states than for the optimal product. This is a tedious process which would be impractical even if (a) holds in higher dimensions, Nevertheless, it gives some insight and is reminiscent of the argument used in [22].

The next example exploits the isomorphism  $\mathbf{C}_4 \simeq \mathbf{C}_2 \otimes \mathbf{C}_2$  to show that decomposability is a basis dependent property.

**Example 6** If  $\rho = |v\rangle\langle v|$  with  $\langle v| = (1, 0, 1, 0)$  then  $N^C(\rho)$  is decomposable in the generalized Pauli basis for  $d = 4$ , but *not* is the basis given by products of (the usual) Pauli matrices. If  $\rho = |v\rangle\langle v|$  with  $\langle v| = (1, 0, 0, 1)$  then  $N^C(\rho)$  is *not* decomposable in the generalized Pauli basis for  $d = 4$ , but *is* decomposable in the basis given by products of (the usual) Pauli matrices.

## References

- [1] R. Alicki and M. Fannes, “Note on multiple additivity of minimal output entropy output of extreme  $SU(d)$ -covariant channels” *Open Systems and Information Dynamics* **11**, 339–342 (2004) (quant-ph/0407033).
- [2] M-D Choi, “Completely Positive Linear Maps on Complex Matrices” *Lin. Alg. Appl.* **10**, 285–290 (1975).



- [3] J. Cortese, “The Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels” (quant-ph/0211093).
- [4] I. Devetak and P. W. Shor, “The capacity of a quantum channel for simultaneous transmission of classical and quantum information” *Commun. Math. Phys.* **256**, 287–303 (2005). quant-ph/0311131
- [5] G. Vidal, W. Dür, and J. I. Cirac, “Entanglement Cost of Bipartite Mixed States” *Phys. Rev. Lett.* **89**, 027901 (2002).
- [6] A. Fujiwara and T. Hashizumé, “Additivity of the capacity of depolarizing channels” *Phys Lett. A* , **299**, 469–475 (2002).
- [7] M. Fukuda, “Extending additivity from symmetric to asymmetric channels” *J. Phys. A* quant-ph/0505022.
- [8] M. Fukuda and A.S. Holevo, “On Weyl-covariant channels” quant-ph/0510148
- [9] V. Giovannetti and S. Lloyd, “Additivity properties of a Gaussian channel” *Phys. Rev. A*, **69**, 062307 (2004).
- [10] V. Giovannetti, S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen, “Minimum Rényi and Wehrl entropies at the output of bosonic channels” *Phys. Rev. A* **70**, 022328 (2004) (quant-ph/0404037).
- [11] V. Giovannetti, S. Lloyd and M. B. Ruskai, “Conditions for multiplicativity of maximal  $l_p$ -norms of channels for fixed integer  $p$ ”, *J. Math. Phys.* **46**, 042105 (2005) (quant-ph/0408103).
- [12] A. S. Holevo, “Coding Theorem for Quantum Channels” quant-ph/9809023; “Quantum coding theorems”, *Russian Math. Surveys* **53** 1295–1331 (1999).
- [13] A. S. Holevo, “Remarks on the classical capacity of quantum channel” (quant-ph/0212025).
- [14] A. S. Holevo, “On complementary channels and the additivity problem” quant-ph/0509101
- [15] R.A. Horn and C.R. Johnson, *Matrix Analysis* (Cambridge University Press, 1985).
- [16] M. Horodecki, P. Shor, and M. B. Ruskai, “Entanglement Breaking Channels” *Rev. Math. Phys* **15**, 629–641 (2003) (quant-ph/030203).

- [17] C. King, “Maximization of capacity and p-norms for some product channels”, *J. Math. Phys.*, **43** 1247 – 1260 (2002).
- [18] C. King, “Additivity for unital qubit channels”, *J. Math. Phys.*, **43** 4641 – 4653 (2002).
- [19] C. King, “The capacity of the quantum depolarizing channel”, *IEEE Transactions on Information Theory*, **49**, 221 – 229, (2003).
- [20] C. King, “Maximal p-norms of entanglement breaking channels”, *Quantum Information and Computation*, **3**, 186–190 (2003).
- [21] C. King, “An application of the Lieb-Thirring inequality in quantum information theory”, to appear in Proceedings of ICMP 2003.
- [22] C. King and M. B. Ruskai, “Minimal Entropy of States Emerging from Noisy Quantum Channels”, *IEEE Trans. Info. Theory*, **47**, 192–209 (2001).
- [23] K. Kraus, “General state changes in quantum theory” *Ann. Physics* **64**, 311–335 (1971); *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer-Verlag, 1983).
- [24] D. Kretschmann and R. F. Werner “Quantum Channels with Memory” quant-ph/0502106
- [25] L. J. Landau and R. F. Streater, “On Birkhoff’s theorem for doubly stochastic completely positive maps of matrix algebras”, *Linear Algebra and its Applications*, **193**, 107–127 (1993).
- [26] G. Lindblad “Completely Positive Maps and Entropy Inequalities” *Commun. Math. Phys.* **40**, 147–151 (1975).
- [27] A.W. Marshall and I. Olkin, *Inequalities: Theory of majorization and its applications* (Academic Press, 1979).
- [28] K. Matsumoto, T. Shiono and A. Winter, “Remarks on additivity of the Holevo channel capacity and of the entanglement of formation” *Commun. Math. Phys.* **246**, 427–442 (2004).
- [29] V. Paulsen, *Completely Bounded Maps and Operator Algebras* (Cambridge University Press, 2002).
- [30] G. W. Ritter, “Quantum Channels and Representation Theory” *J. Math. Phys.* **46**, (2005) (quant-ph/0502153).

- [31] M. B. Ruskai, S. Szarek, E. Werner, “An analysis of completely positive trace-preserving maps  $M_2$ ” *Lin. Alg. Appl.* **347**, 159 (2002).
- [32] M. B. Ruskai, in preparation.
- [33] P. Shor, “Additivity of the classical capacity of entanglement-breaking quantum channels” *J. Math. Phys.* **43**, 4334–4340 (2002).
- [34] P. W. Shor, “Equivalence of Additivity Questions in Quantum Information Theory”, *Commun. Math. Phys.* **246**, 453– 472 (2004) (quant-ph/0305035).
- [35] W.F. Stinespring, “Positive functions on  $C^*$ -algebras” *Proc. Amer. Math. Soc.* **6**, 211–216 (1955).
- [36] R. F. Werner and A. S. Holevo, “Counterexample to an additivity conjecture for output purity of quantum channels”, *J. Math. Phys.* **43**, no. 9, 4353 – 4357 (2002).
- [37] A. Winter, “On environment-assisted capacities of quantum channels” (quant-ph/0507045).
- [38] M.M. Wolf and J. Eisert “Classical information capacity of a class of quantum channels” (quant-ph/0412133).